Attorney's Docket No. 413-010736-US(PAR) ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Express Mail No.: EL627511287US
Applicant(s): Jari VALLSTROM **Group No.:**
Serial No.: 0 /
Filed: Herewith **Examiner:**
For: SMART CARD OF A TERMINAL, A TERMINAL USING A SMART CARD, AND AN IMPROVED METHOD FOR IDENTIFYING A USER BY MEANS OF A SMART CARD

Commissioner of Patents
Washington, D.C. 20231

TRANSMITTAL OF CERTIFIED COPY

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

Country : Finland
Application Number : 20002813
Filing Date : December 21, 2000

WARNING: "When a document that is required by statute to be certified must be filed, a copy, including a photocopy or facsimile transmission of the certification is not acceptable." 37 CFR 1.4(f) (emphasis added.)

SIGNATURE OF ATTORNEY

Reg. No.: 24,622

Clarence A. Green

Type or print name of attorney

Tel. No.: (203) 259-1800

Perman & Green, LLP

P.O. Address

Customer No.: 2512

425 Post Road, Fairfield, CT 06430

NOTE: The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63.

NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 6.11.2001

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija Applicant	**Nokia Mobile Phones Ltd** **Espoo**
Patenttihakemus nro Patent application no	**20002813**
Tekemispäivä Filing date	**21.12.2000**
Kansainvälinen luokka International class	**H04Q**

Keksinnön nimitys
Title of invention

"Päätelaitteen älykortti, älykorttia käyttävä päätelaite ja parannettu menetelmä käyttäjän tunnistamiseksi älykorttia käyttämällä"

Tätten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1782/1995 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1782/1995 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A, P.O.Box 1160, FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

L2

Päätelaitteen älykortti, älykorttia käyttävä päätelaite ja parannettu menetelmä käyttäjän tunnistamiseksi älykorttia käyttämällä

Keksinnön kohteena on tiedonsiirtoverkon päätelaitteeseen asennettava SIM-kortti. Keksinnön kohteena on myös tiedonsiirtoverkon päätelaite, joka on järjestetty suorittamaan käyttäjän tunnistus päätelaitetta käyttöönotettaessa. Samoin keksinnön kohteena on menetelmä yksittäisen päätelaitteen käyttäjän tunnistamiseksi tiedonsiirtoverkon päätelaitteeseen asennetussa SIM-kortissa henkilökohtaisen tunnusluvun perusteella.

Useissa erilaisissa solukkojärjestelmissä käytetään erilaisia menetelmiä päätelaitteen käyttäjän tunnistamiseksi. Alimman tasoisena tunnistuksena voidaan pitää menettelyä, jolla tunnistetaan jonkun käyttäjän oikeus käyttää jotakin solukkojärjestelmän päätelaitetta. Tämä tunnistus tehdään esimerkiksi käyttämällä ns. PIN-koodia (Personal Identification Number). PIN-koodi on useamman numeron pituinen koodi, jonka oikea syöttö laitteeseen sallii käyttäjän käyttää kyseistä päätelaitetta. Esimerkiksi eri järjestelmissä käytettävät solukkopuhelimet vaativat muutaman numeron PIN-koodin, jotta päätelaitteen puhelinominaisuudet saataisiin käyttöön. Ainoastaan hätänumeroon osoitettu soitto ei vaadi PIN-koodin käyttöä. Solukkopuhelimessa, kuten esimerkiksi GSM:ssä (Global System for Mobile communications) toimivassa solukkopuhelimessa, tämä tunnistetoiminto on sisällytetty erilliseen mutta päätelaitteeseen liitettävissä olevaan SIM-korttiin (Subscriber Identity Module). Yleensä jokaisella solukkoverkon päätelaitteen käyttäjällä on oma, henkilökohtainen SIM-korttinsa, jonka hän kytkee siihen solukkoverkon päätelaitteeseen, jota hän haluaa käyttää. Kun käyttäjä näppäilee oman PIN-tunnisteensa päätelaitteeseen, tekee SIM-kortilla oleva prosessori vertailun annetun PIN-tunnisteen ja muistissaan olevan tietylle käyttäjälle tarkoitetun PIN-tunnisteen välillä. Mikäli tunnistetoiminto antaa positiivisen tuloksen, sallitaan käyttäjän pääsy laitteen muihin toimintoihin. Tunnetaan myös ratkaisuja, joissa samaan solukkoverkon päätelaitteeseen on asennettavissa ainakin kaksi erillistä SIM-korttia, joilla voi olla erilaiset PIN-tunnistekoodit.

SIM-kortti voi pitää sisällään lisäksi muita käyttäjäkohtaisia tietoja, jotka voivat sallia käyttäjän toimivan solukkoverkossa tai edesauttaa sitä. Tällaisia tietoja ovat mm. erilaiset tiedonsiirron salauksessa käytettävät julkiset tai salaiset salakirjoitusavaimet ja käyttäjän autentikoinnissa käytettävät menettelyt.

On myös olemassa solukkojärjestelmiä, joissa voidaan ainakin olettaa useiden eri käyttäjien voivan joutua käyttämään samoja päätelaitteita. Tällaisia järjestelmiä käyttävät ainakin eri viranomaiset kuten poliisi, palokunta ja muut pelastusalan viranomaiset. Tällä hetkellä käytössä olevat järjestelmät ovat yleensä analogisella tekniikalla toteutettuja, huonosti salattuja ja toistensa kanssa yhteensopimattomia. Yhteistä viranomaisten käyttöön tulevaa ylikansallista, aikajakoista ja digitaalista solukkopuhelinjärjestelmää TETRAa (Terrestial Trunked Radio) ollaan paraikaa luomassa. Järjestelmän standardointityötä tekee ETSI (European Telecommunications Institute). TETRA-verkon tulee yhtä aikaa olla kaikille viranomaisille helppokäyttöinen ja myös tietoturvallisuuden kannalta hyvin salattu. Periaatteessa eri maiden viranomaiset ovat liitettävissä samaan TETRA-verkkoon. TETRA-verkon päätelaitteiden sisältämiä, tunnistuksessa käytettäviä PIN-koodeja ja muita mahdollisesti tarvittavia salasanoja ei saa päästää leviämään käyttäjäkunnan ulkopuolelle.

Ongelmaksi tällaisessa päätelaitteiden yhteiskäytössä on kuitenkin muodostunut se, että käyttäjien tulee pitää muistissaan erilaisia tunnistuskoodeja useita kappaleita, koska he eivät useinkaan tiedä, mitä päätelaitetta käyttävät seuraavassa työvuorossa. Niinpä usein päätelaitteen tunnistetiedot ja erilaiset salasanat liitetään ei-sallituilla menetelmillä päätelaitteen yhteyteen, jotta päätelaite yleensä saataisiin tarvittaessa nopeasti toimimaan. Laitteen tuntema PIN-koodi voidaan esimerkiksi kirjoittaa laitteen takapuolelle joko laitteen kuoreen tai johonkin laitteeseen liimattuun muistilappuun. Käyttäjä voi myös tallentaa useiden päätelaitteiden tunnistetiedot erilliselle muistilapulle. Tällä tavoin voivat jonkin päätelaitteen käyttöön liittyvät tunnistetiedot joutua asiattomiin käsiin, ja turvallisen ja salatun viranomaisverkon toiminta vaarantuu. Tietovuotojen mahdollisuuden takia on joissakin järjestelmissä käytössä PIN-koodien ja muiden salasanojen nopeutettu kierto. Tämä taas voi johtaa entistä todennäköisemmin siihen, että käyttäjät kirjoittavat salasanat ylös muistilapulle, mikä ei ole luonnollisesti toivottavaa.

Esillä olevan keksinnön tavoitteena on esittää laite, menettely ja järjestely, jonka avulla voidaan monen käyttäjän ympäristössä turvata sekä päätelaitteen käytön turvallisuus että päätelaitteen käyttöönoton helppous.

Keksinnön tavoitteet saavutetaan solukkoverkon päätelaitteeseen sijoitettavalla SIM-kortilla, jonka yhteyteen on tallennettu käyttäjäkohtaista tunnistetietoa kutakin mahdollista käyttäjää varten.

Keksinnön mukaiselle SIM-kortille on tunnusomaista, että SIM-kortti käsittää välineet ainakin kahden käyttäjän tunnistamiseen käytettävien tietojen tallentamiseksi ja välineet käyttäjän tunnistuksen tekemiseksi mainittuja tietoja käyttämällä.

Keksinnön mukaiselle päätelaitteelle on tunnusomaista, että päätelaitteen välineet käyttäjän tunnistamiseksi käsittävät SIM-kortin, joka on järjestetty tunnistamaan ainakin kaksi tai useampi päätelaitteen käyttöön oikeutettu käyttäjä ainakin yhden käyttäjäkohtaisen tunnuskoodin avulla.

Keksinnön mukaiselle menetelmälle on tunnusomaista, että käyttäjän tunnistaminen suoritetaan vertaamalla päätelaitteen käyttäjän antamaa tunnuskoodia päätelaitteen SIM-korttiin tallennettuihin, eri käyttäjille varattuihin tunnuskoodeihin, ja mikäli päätelaitteen käyttäjän antama tunnuskoodi on näiden mainittujen tunnuskoodien joukossa, sallitaan päätelaitteen käyttöönotto.

Keksinnön eräitä edullisia suoritusmuotoja on esitetty epäitsenäisissä patenttivaatimuksissa.

Keksinnön perusajatus on seuraava: Solukkojärjestelmän päätelaitteeseen asennetaan SIM-kortti, johon on tallennettu useita, eri käyttäjille tarkoitettuja PIN-koodeja. Tällöin kunkin käyttäjän tarvitsee tuntea ainoastaan oma PIN-koodinsa riippumatta siitä, minkä päätelaitteen hän saa käyttöönsä. PIN-tunnistuksen lisäksi voidaan käyttäjältä vaatia jokin toinenkin lisätunniste/salasana, joka päästää käyttäjän hyödyntämään päätelaitetta. Erillisten PIN-koodien lisäksi voidaan SIM-korttiin tallentaa erilaisia muita salauksessa ja tiedonsiirrossa käytettäviä käyttäjäkohtaisia tietoja. Nämä käyttäjäkohtaiset tiedot voivat olla ainoastaan kulloisenkin tunnistetun käyttäjän hyödynnettävissä.

Keksinnön etuna on, että yhteiskäytössä oleviin solukkoverkon päätelaitteisiin tarvitsee asentaa ainoastaan yksi SIM-kortti, jota kukin käyttäjä voi hyödyntää omalla tuntemallaan PIN-koodilla/lisätunnisteella.

Lisäksi keksinnön etuna on, että yhteiskäytössä olevan päätelaitteen käyttöönotto helpottuu, koska se saadaan käyttökuntoon kunkin henkilön tuntemalla tunnuskoodilla.

Edelleen keksinnön etuna on, että yhteen SIM-korttiin voidaan käyttäjäkohtaisesti tallentaa myös muuta kutakin käyttäjää koskevaa tietoa, jota voidaan käyttää hyväksi tiedonsiirtoyhteyden/istunnon aikana.

Seuraavassa keksintöä selostetaan yksityiskohtaisesti. Selostuksessa viitataan oheisiin piirustuksiin, joissa

kuva 1 esittää esimerkinomaisesti keksinnön mukaisen SIM-kortin eräitä pääosia,

kuva 2 esittää esimerkinomaisesti SIM-kortilla olevaa käyttäjäkohtaista tietorakennetta,

kuva 3 esittää esimerkinomaisena vuokaaviona keksinnön mukaisen SIM-kortin mahdollistavaa käyttäjän tunnistamistoimintaa ja

kuva 4 esittää esimerkinomaisesti keksinnön mukaista SIM-korttia hyödyntävää solukkoverkon päätelaitetta.

Kuvassa 1 on esitetty esimerkinomaisesti johonkin solukkoverkon päätelaitteeseen asetettuun SIM-korttiin 10 kuuluvia keksinnön mukaisia pääosia. Keksinnön mukaisessa SIM-kortissa on varattu käyttäjäkohtaisten tietojen tallennustilaa useita käyttäjiä 1, 2,...N varten. Kukin käyttäjäkohtainen tietue 11a, 11b, 11c on yhteyden 14 avulla kytketty SIM-korttiin kuuluvaan liitäntäyksikköön 12. Liitäntäyksikön 12 avulla SIM-kortti on sähköisesti kytkettävissä tarvittaviin päätelaitteen sähköisiin kytkentöihin. Liitäntäyksikön 12 kautta SIM-korttiin syötetään ne tunnistetiedot/tunnuskoodit ja tunnuskoodikyselyt, jotka antavat tietylle käyttäjälle luvan kyseisen päätelaitteen käyttöön. Lisäksi SIM-kortilla on edullisesti kaikkien päätelaitteen käyttäjien yhteiseen käyttöön tarkoitettu tietue, viite 15. Käyttäjäkohtaisten tietueiden määrää rajoittaa ainoastaan kyseisen SIM-kortin muistikapasiteetti.

Kuvassa 2 on esitetty esimerkinomaisesti, mitä tietoja käyttäjäkohtainen tietue 11a, 11b, 11c edullisesti pitää sisällään. Kukin tietueista sisältää edullisesti ainakin yhden käyttäjäkohtaisen PIN-koodin, viite 21. Käytössä voi luonnollisesti olla myös useita erilaisia PIN-koodeja kutakin käyttäjää varten. Kyseisillä PIN-koodeilla sallitaan erilaisia toimintoja kyseiselle päätelaitteen käyttäjälle. Käyttäjäkohtaisesti on myös edullista tallentaa ainakin yksi PUK-koodi (Personal Unblockin Code), viite 22. Tällä koodilla estetään PIN-koodin murtaminen pelkästään kokeilemalla, sillä kun PIN-koodeja on kokeiltu tietty määrä, SIM-kortti vaatii tämän pitemmän koodin, jotta päätelaite saataisiin käyttöön. Jos PUK-koodin antaa useamman kerran väärin, lukkiutuu SIM-kortti, ja laite on hätäpuhelua lukuun ottamatta käyttökelvoton. Lisäksi SIM-korttiin on tallennettu edullisesti myös muita käyttäjäkohtaisia salasanoja, viite 23, jotka on mahdollisesti tiedettävä solukkoverkon päätelaitetta käyttöönotettaessa.

Keksinnön mukaiseen TETRA-solukkoverkossa käytettävään SIM-korttiin voi kuulua edullisesti myös TETRA-järjestelmän käyttäjän identifioiva tunniste ITSI (Individual TETRA Subscriber Identification), viite 24. Tätä tietoa tarvitaan TETRA-verkon liikennöinnissä kulloisenkin käyttäjän tunnistukseen.

Samoin keksinnön mukainen SIM-kortti käsittää edullisesti käyttäjän solukkoverkkoon kytkeytymisen yhteydessä tarvittavan autentikointiavaimen, viite 25. SIM-kortti käsittää lisäksi edullisesti liikenteen salaamisessa käytettäviä erilaisia salausavaimia, viite 26, jotka on edullista tallentaa SIM-kortille käyttäjäkohtaisena tietona.

Keksinnön mukaiseen SIM-korttiin on edullisesti tallennuttuna myös muuta käyttäjäkohtaista tietoa, viite 27, josta on verkon toiminnan tai käyttäjän kannalta hyötyä.

Kuvassa 3 on esitetty esimerkinomaisena vuokaaviona, miten keksinnön mukaista SIM-korttia voidaan hyödyntää TETRA-solukkoverkon päätelaitteessa. Lähtötilanteessa päätelaitteeseen on kytkettynä SIM-kortti, joka sisältää usean käyttäjän käyttäjäkohtaisia tietueita 11a, 11b, 11c. Vaiheessa 31 päätelaitteeseen kytketään virta. Kun virta on saatu kytkettyä, käyttäjälle esitetään PIN-koodikysely, johon päätelaitteen käyttäjän on vastattava antamalla tuntemansa PIN-koodi, vaihe 32. Vaiheessa 33 tehdään päätelaitteen käyttäjän antaman PIN-koodin vertailu SIM-korttiin 10 tallennettuun tietoon. Vaiheessa 34 tehdään päätös siitä, hyväksytäänkö päätelaitteen käyttäjän antama PIN-koodi vai ei. Mikäli PIN-koodia ei hyväksytä, pyydetään PIN-koodia edullisesti uudelleen eli palataan vaiheeseen 32. Tähän takaisinkytkentään vaiheesta 34 vaiheeseen 32 on mahdollista sisällyttää myös kuvassa 3 esittämätön PIN-koodien yrityskertojen laskutoiminto, jossa laskutoiminnossa ennalta määrättyjen yrityskertojen ylittämisen jälkeen tarvitaan PUK-koodin syöttäminen päätelaitteeseen, jotta toimintaa voitaisiin jatkaa.

Varsinaisen PIN-koodin hyväksymisen jälkeen voidaan käyttäjältä vaatia vielä jokin lisätunniste/salasana/tunnuskoodi, vaihe 35. Jos lisätunnistetta ei vaadita, siirrytään vaiheeseen 39, jossa päätelaite on käyttökunnossa. Jos kuitenkin tarvitaan lisätunnisteen/käyttäjäkohtaisen salasanan hyväksyntä, siirrytään vaiheesta 35 vaiheeseen 36. Vaiheessa 36 käyttäjä antaa tuntemansa lisätunnisteen/salasanan. Vaiheessa 37 suoritetaan päätelaitteen käyttäjän antaman lisätunnisteen/salasanan vertailu käyttäjäkohtaiseen SIM-kortin muistissa olevaan lisätunnisteeseen/salasanaan 23. Jos käyttäjän antama lisätunniste/salasana on hyväksyttävissä, niin vaiheesta 38 siirrytään vaiheeseen 39, jossa päätelaite on käyttökunnossa. Jos vaiheessa 38 todetaan, ettei annettu lisätunniste/salasana vastaa SIM-kortin muistiin taltioitua tietoa 27, palataan vaiheeseen 36, jossa käyttäjää pyydetään uudestaan antamaan tuntemansa

lisätunniste/salasana. Tähän takaisinkytkentään vaiheesta 38 vaiheeseen 36 on mahdollista sisällyttää myös kuvassa 3 esittämätön lisätunnisteen/salasanan yrityskertojen laskutoiminto, jossa laskutoiminnossa ennalta määrätyn yrityskertojen ylittämisen jälkeen tarvitaan PUK-koodin syöttäminen, jotta toimintaa voitaisiin jatkaa.

Eräässä keksinnön mukaisessa suoritusmuodossa kysytään käyttäjältä PIN-koodi ja myös lisätunnus vaiheessa 32 ennen PIN-koodille suoritettavaa testausta. Tässä suoritusmuodossa siirrytään vaiheesta 34 suoraan vaiheeseen 37, mikäli PIN-koodivertailu 34 antaa hyväksyttävän tuloksen. Luonnollisesti PIN-koodivertailun 34 ja lisätunnusvertailun 37 järjestys voidaan vaihtaa ilman, että se vaikuttaa tunnistusrutiinin lopputulokseen.

Kuva 4 esittää yksinkertaistettuna lohkokaaviona erästä keksinnön mukaista päätelaitetta 400. Päätelaite käsittää antennin 401 radiotaajuisten signaalien eli RF-signaalien vastaanottamiseksi ja lähettämiseksi. Vastaanotettu RF-signaali ohjataan kytkimellä 402 RF-vastaanottimeen 411, jossa signaali vahvistetaan ja muunnetaan digitaaliseksi. Tämän jälkeen signaali ilmaistaan ja demoduloidaan lohkossa 412. Lohkossa 413 suoritetaan salauksen ja lomituksen purku. Tämän jälkeen suoritetaan signaalinkäsittely lohkossa 430. Vastaanotettu data voidaan sellaisenaan tallentaa matkaviestimen muistiin 404 tai vaihtoehtoisesti käsitelty pakettidata siirretään signaalinkäsittelyn jälkeen mahdolliseen ulkoiseen laitteeseen, kuten tietokoneeseen. Ohjausyksikkö 403 suorittaa em. vastaanottolohkojen ohjauksen ohjausyksikköön tallennetun ohjelman mukaisesti.

Lähetystoiminto päätelaitteesta tapahtuu esim. seuraavasti. Ohjausyksikön 403 ohjaamana lohko 433 suorittaa datalle mahdollisen signaalinkäsittelyn ja lohko 421 suorittaa käsitellylle, siirrettävälle signaalille lomituksen ja salauksen. Koodatusta datasta muodostetaan purskeet, lohko 422, jotka moduloidaan ja vahvistetaan lähetettäväksi RF-signaaliksi lohkossa 423. Lähetettävä RF-signaali siirretään antenniin 401 kytkimen 402 välityksellä. Myös edellä mainittuja käsittely- ja lähetystoimintoja ohjaa ohjausyksikkö 403.

Kuvan 4 esittämässä päätelaitteessa keksinnön kannalta oleellinen osa on laitteeseen asennettu SIM-kortti 405. Tähän SIM-korttiin on tallennettu niin kaikki käyttäjäkohtaiset tiedot kuin myös kaikkien yhteiset päätelaitteen käytössä tarvittavat tiedot. Lisäksi keksinnön mukaisessa päätelaitteessa hyödynnetään päätelaitteeseen kuuluvaa näyttöä 432 sekä näppäimistöä 431. Kaikki SIM-kortin vaatimat tunnuskoodit syötetään päätelaitteeseen edullisesti kyseisen näppäimistön avulla.

Keksintö ei sinällään aseta TETRA-solukkoverkon tukiasemille, joita ei ole esitetty kuvassa 4, erillisiä vaatimuksia verrattuna käytössä olevaan tekniikan tasoon.

Edellä on kuvattu eräitä keksinnön mukaisia suoritusmuotoja. Keksintö ei rajoitu juuri kuvattuihin suoritusmuotoihin. Esimerkiksi PIN-koodin ja muiden tunnisteiden kyselyjärjestys voi olla jokin muu kuin selityksessä esitetyn esimerkin mukainen järjestys. Samoin keksinnön mukainen SIM-kortti voi edullisesti sisältää muitakin tietoja kuin selityksen esimerkinomaisten suoritusmuotojen sisältämät tiedot. Lisäksi keksintö ei rajoitu esimerkkinä esitetyn TETRA-solukkoverkon päätelaitteeseen. Lisäksi päätelaite voi olla myös jonkin kiinteän verkon päätelaite. Keksinnöllistä ajatusta voidaan soveltaa lukuisilla tavoilla patenttivaatimusten asettamissa rajoissa.

Patenttivaatimukset

1. Tiedonsiirtoverkon päätelaitteeseen asennettava SIM-kortti (10), **tunnettu** siitä, että SIM-kortti käsittää välineet ainakin kahden käyttäjän tunnistamiseen käytettävien tietojen (11a, 11b, 11c) tallentamiseksi ja välineet käyttäjän tunnistuksen tekemiseksi mainittuja tietoja käyttämällä.

2. Patenttivaatimuksen 1 mukainen SIM-kortti, **tunnettu** siitä, että SIM-kortti käsittää lisäksi välineet kaikkien mainitun päätelaitteen käyttäjien yhteisesti hyödyntämien tietojen (15) tallentamiseksi.

3. Patenttivaatimuksen 1 mukainen SIM-kortti, **tunnettu** siitä, että mainitut käyttäjän tunnistamiseen tarvittavat tiedot (11a, 11b, 11c) käsittävät ainakin yhden käyttäjäkohtaisen tunnuskoodin.

4. Patenttivaatimuksen 3 mukainen SIM-kortti, **tunnettu** siitä, että mainitut käyttäjän tunnistamiseen tarvittavat tiedot (11a, 11b, 11c) käsittävät ainakin yhden seuraavista koodeista: käyttäjäkohtainen PIN-koodi (21), käyttäjäkohtainen PUK-koodi (22).

5. Patenttivaatimuksen 3 mukainen SIM-kortti, **tunnettu** siitä, että mainitut käyttäjän tunnistamiseen tarvittavat tiedot (11a, 11b, 11c) käsittävät lisäksi ainakin yhden käyttäjäkohtaisen salasanan (23).

6. Patenttivaatimuksen 3 mukainen SIM-kortti, **tunnettu** siitä, että mainitut käyttäjän tunnistamiseen tarvittavat tiedot (11a, 11b, 11c) käsittävät lisäksi ainakin yhden käyttäjäkohtaisen ITSI-koodin (24).

7. Patenttivaatimuksen 1 mukainen SIM-kortti, **tunnettu** siitä, että SIM-kortti käsittää lisäksi ainakin yhden käyttäjäkohtaiseen autentikointiin käytetyn salausavaimen (25).

8. Patenttivaatimuksen 1 mukainen SIM-kortti, **tunnettu** siitä, että SIM-kortti käsittää lisäksi yhteyden salaamisessa käytettävät käyttäjäkohtaiset salausavaimet (26).

9. Patenttivaatimuksen 1 mukainen SIM-kortti, **tunnettu** siitä, että SIM-kortti käsittää lisäksi muuta päätelaitteen käytössä tarvittavaa käyttäjäkohtaista tietoa (27).

10. Jokin edellisten patenttivaatimusten mukainen SIM-kortti, **tunnettu** siitä, että mainittu SIM-kortti on järjestetty käytettäväksi viranomaisverkon päätelaitteessa.

11. Solukkoverkon päätelaite (400), joka on järjestetty suorittamaan käyttäjän tunnistus päätelaitetta käyttöönotettaessa, **tunnettu** siitä, että välineet käyttäjän tunnistamiseksi käsittävät SIM-kortin (405), joka on järjestetty tunnistamaan ainakin kaksi päätelaitteen käyttöön oikeutettua käyttäjää ainakin yhden käyttäjäkohtaisen tunnuskoodin avulla.

12. Patenttivaatimuksen 11 mukainen päätelaite (400), **tunnettu** siitä, että päätelaite on järjestetty käytettäväksi viranomaisverkossa.

13. Patenttivaatimuksen 12 mukainen päätelaite, **tunnettu** siitä, että viranomaisverkko on TETRA-solukkoverkko.

14. Menetelmä yksittäisen päätelaitteen käyttäjän tunnistamiseksi tiedonsiirtoverkossa, jossa päätelaitteen käyttäjä tunnistetaan henkilökohtaisen tunnuskoodin perusteella, **tunnettu** siitä, että käyttäjän tunnistaminen suoritetaan vertaamalla päätelaitteen käyttäjän antamaa tunnuskoodia (32) päätelaitteen SIM-korttiin tallennettuihin, eri käyttäjille varattuihin tunnuskoodeihin (33, 34), ja mikäli päätelaitteen käyttäjän antama tunnuskoodi on näiden mainittujen tunnuskoodien joukossa, sallitaan päätelaitteen käyttöönotto.

15. Patenttivaatimuksen 14 mukainen menetelmä, **tunnettu** siitä, että mainittuna käyttöön oikeuttavana tunnuskoodina käytetään henkilökohtaista PIN-koodia.

16. Patenttivaatimuksen 14 mukainen menetelmä, **tunnettu** siitä, että menetelmä käsittää lisäksi vaiheen, jossa päätelaitteen käyttäjältä vaaditaan toinen lisätunniste/salasana (35, 36, 37, 38) päätelaitteen käyttöönottamiseksi.

17. Jokin patenttivaatimusten 14—16 mukainen menetelmä, **tunnettu** siitä, että mikäli päätelaitetta käyttöönottava henkilö antaa mainittuihin tunnuslukukyselyihin väärän tunnusluvun ennalta määrättyä kertaa useammin, on käyttäjän annettava henkilökohtainen PUK-koodi ennen kuin käyttäjän tunnistamista voidaan jatkaa.

(57) Tiivistelmä

Keksinnön kohteena on tiedonsiirtoverkon päätelaitteeseen (400) kytkettävä SIM-kortti (405), joka käsittää välineet ainakin kahden käyttäjän tunnistamiseen tarvittavien tietojen (11a, 11b, 11c) tallentamiseksi ja tunnistuksen tekemiseksi. Keksinnön kohteena on myös mainittua SIM-korttia hyväksikäyttävä solukkoverkon päätelaite. Kyseistä päätelaitetta voivat useat käyttäjät käyttää omilla tunnusluvuillaan ilman, että päätelaitteen SIM-kortti joudutaan vaihtamaan.

Kuva 1

L5

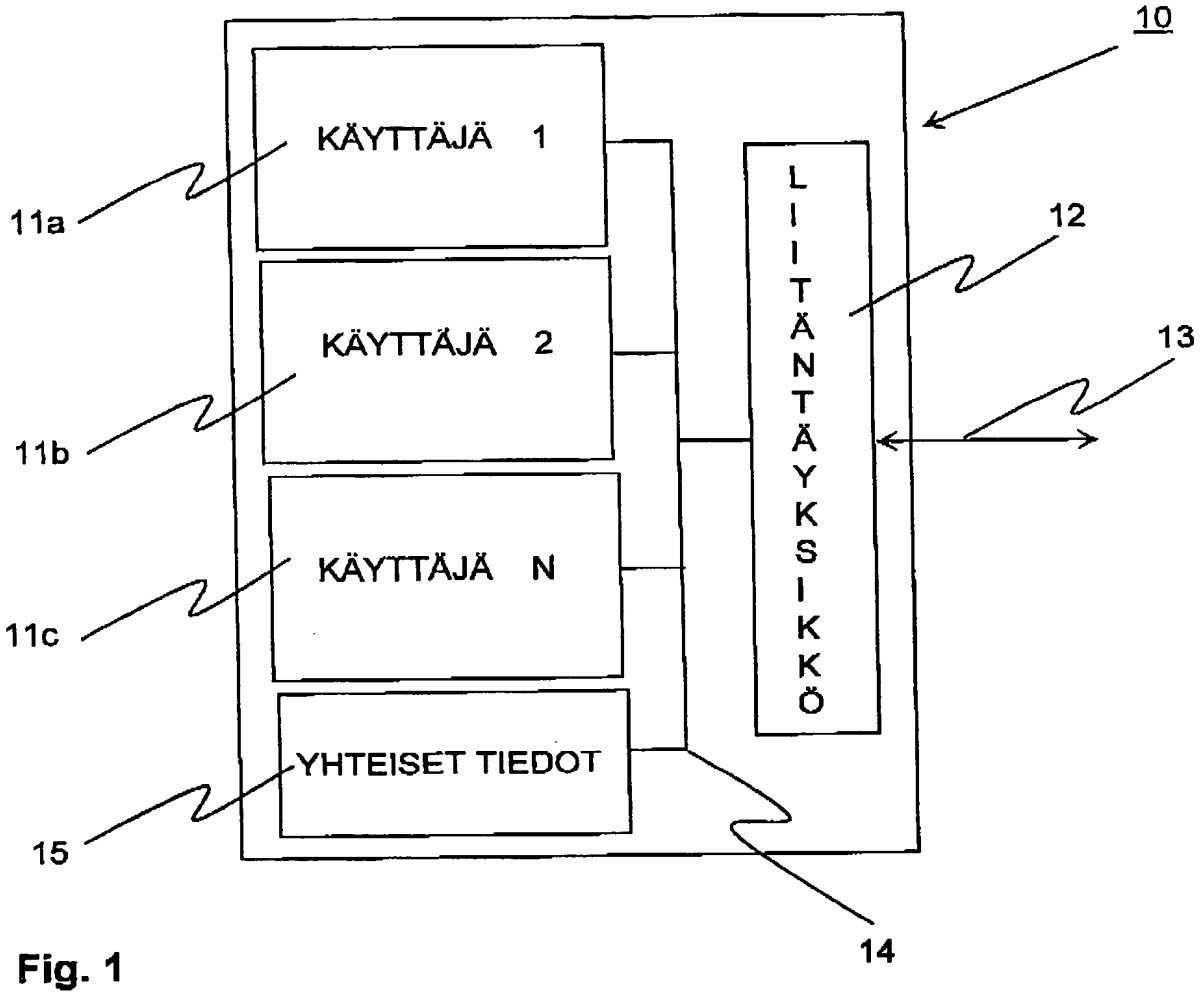
10
KÄYTTÄJÄ 1
KÄYTTÄJÄ 2
KÄYTTÄJÄ N
YHTEISET TIEDOT
LIITÄNTÄYKSIKKÖ
11a
11b
11c
12
13
14
15

Fig. 1

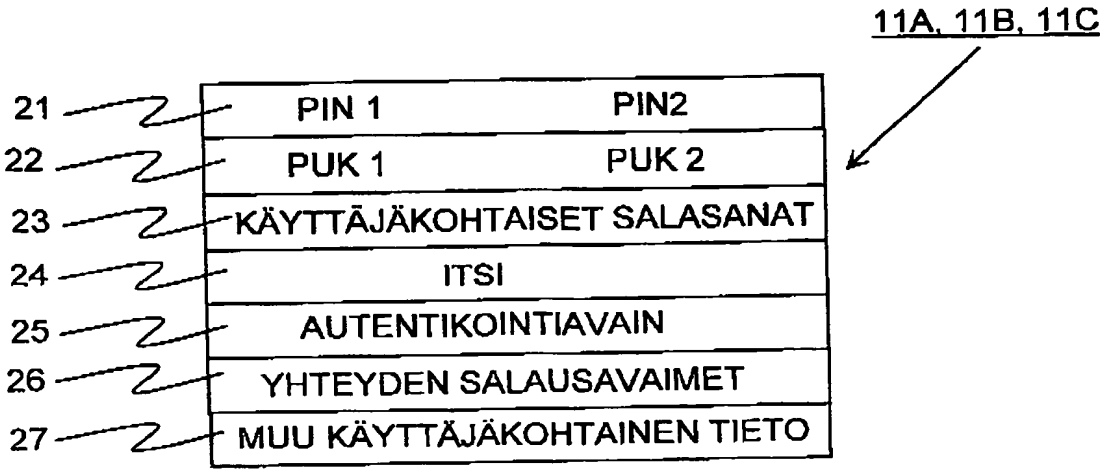
11A, 11B, 11C
21
22
23
24
25
26
27
PIN 1
PIN2
PUK 1
PUK 2
KÄYTTÄJÄKOHTAISET SALASANAT
ITSI
AUTENTIKOINTIAVAIN
YHTEYDEN SALAUSAVAIMET
MUU KÄYTTÄJÄKOHTAINEN TIETO

Fig. 2

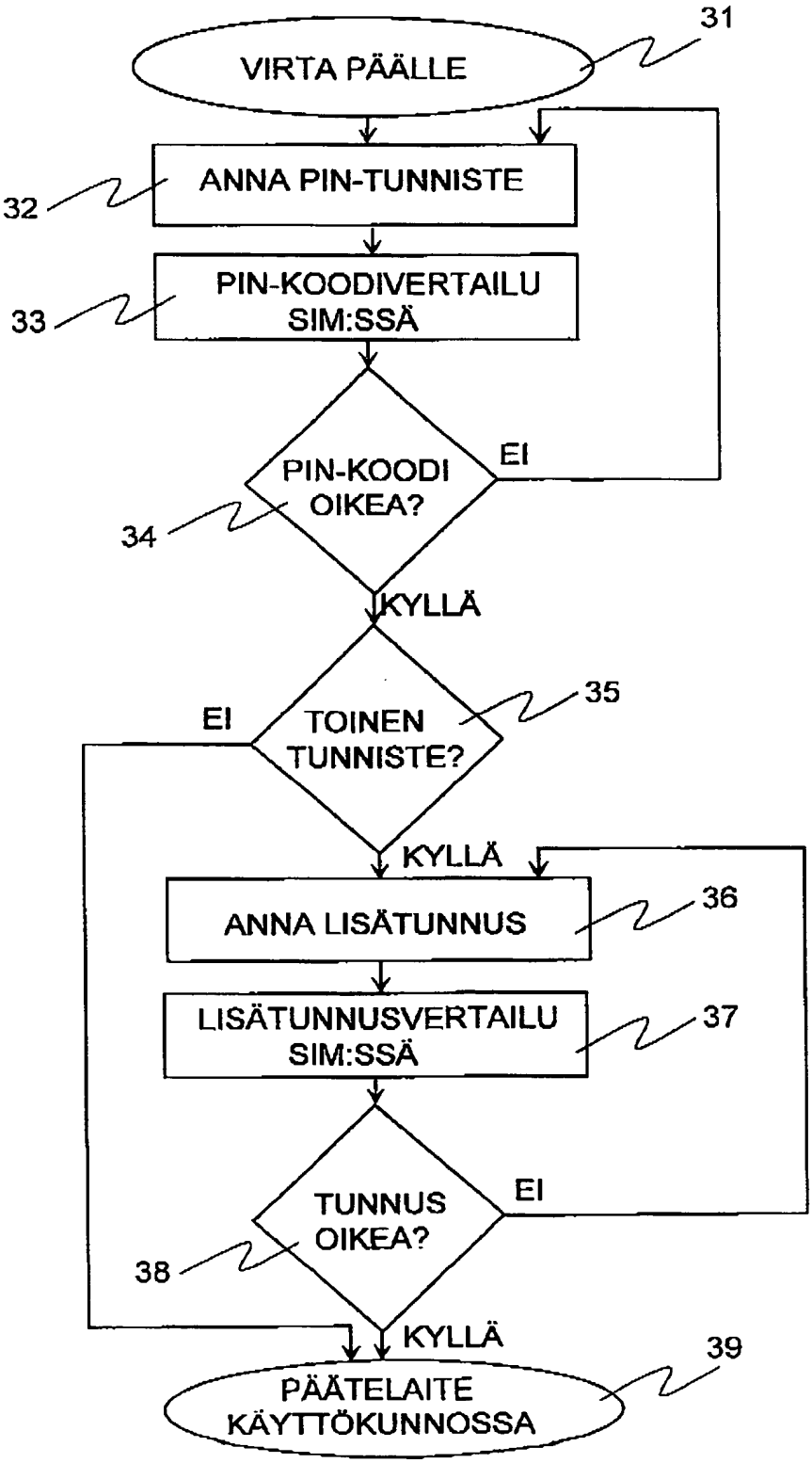
31
VIRTA PÄÄLLE
ANNA PIN-TUNNISTE
32
PIN-KOODIVERTAILU SIM:SSÄ
33
PIN-KOODI OIKEA?
34
EI
KYLLÄ
TOINEN TUNNISTE?
35
EI
KYLLÄ
ANNA LISÄTUNNUS
36
LISÄTUNNUSVERTAILU SIM:SSÄ
37
TUNNUS OIKEA?
38
EI
KYLLÄ
PÄÄTELAITE KÄYTTÖKUNNOSSA
39

Fig. 3

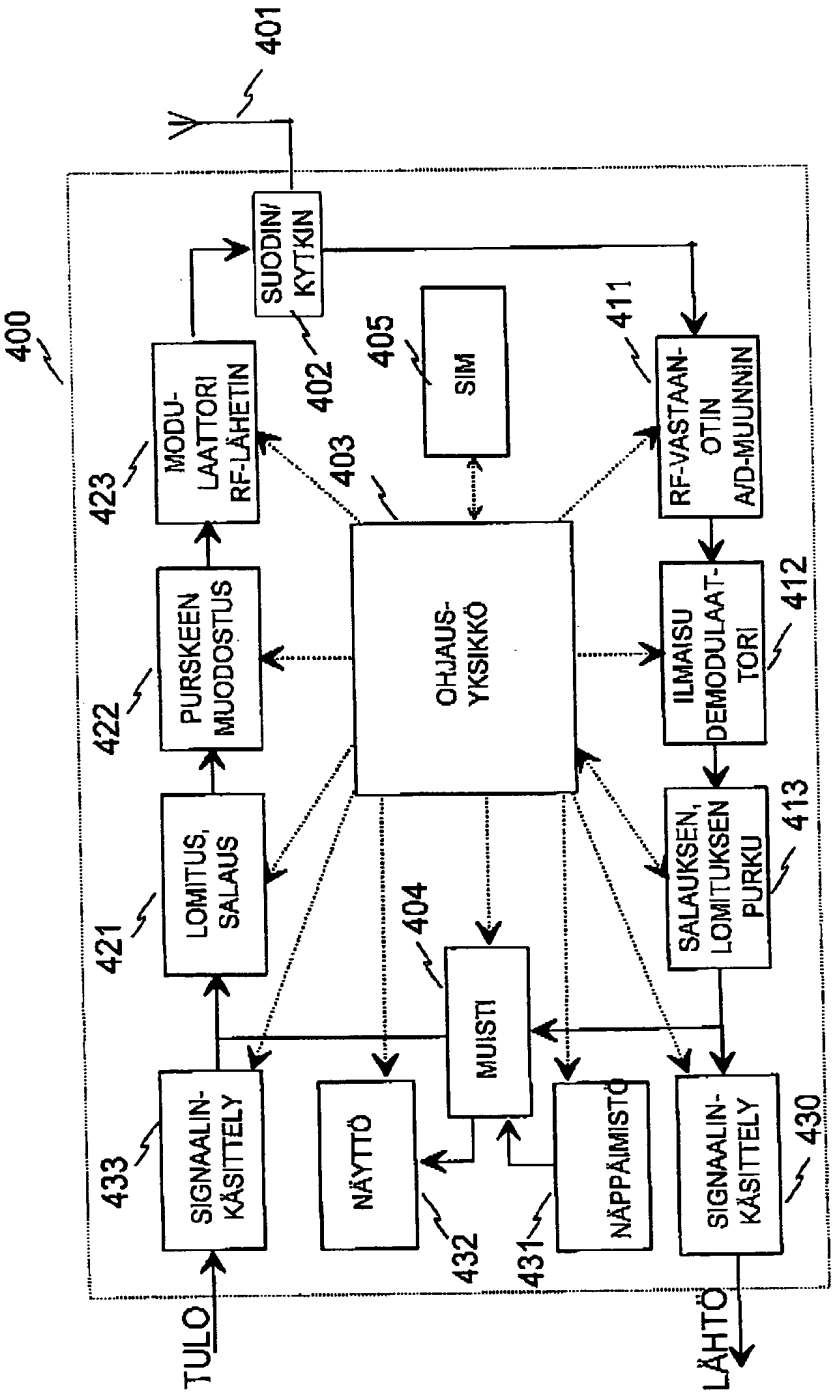
401
400
SUODIN/ KYTKIN
402
405
SIM
411
MODU-LAATTORI RF-LÄHETIN
423
403
RF-VASTAAN-OTIN A/D-MUUNNIN
PURSKEEN MUODOSTUS
422
OHJAUS-YKSIKKÖ
ILMAISU DEMODULAAT-TORI
412
LOMITUS, SALAUS
421
404
SALAUKSEN, LOMITUKSEN PURKU
413
MUISTI
SIGNAALIN-KÄSITTELY
433
NÄYTTÖ
NÄPPÄIMISTÖ
SIGNAALIN-KÄSITTELY
430
432
431
TULO
LÄHTÖ

FIG. 4